

IT Criminal Act*

* Issued by the circular of the Acting Minister of Justice No. 13/T/3087 dated 27.3.1428 AH. pursuant to the Resolution of the Council of Ministers No. 79 dated 7.3.1428 AH. approving the present act.

Article 1

The following words and expressions, wherever they appear in this act, shall have the meanings given opposite to each of them unless the context otherwise requires.

1. Person: Any person of natural, public or private personality.

2. Information System: A set of software and tools prepared for the processing and management of data including computers.

3. Information Network: A link between more than one computer or information system to obtain and exchange data such as private and public networks and the Internet.

4. Data: Information, commands, messages, voices or images that are prepared or have already been prepared for use in computers as well as everything that can be stored, processed, transferred and created by computers such as digits, characters and codes, amongst other things.

5. Software: A set of commands and data that include directions or applications when operated by the computer or computer networks and which performs the required function.

6. Computer: Any fixed or portable wired or wireless electronic system that contains a data processing, storing, transmitting, receiving or browsing system that performs specific functions as per the programmes and commands given to it.

7. Unauthorized Access: The deliberate access of a person to a computer, electronic site, information system or computer network which the said person is unauthorized to access.

8. IT Crime: Any act committed using a computer or information network in violation of the provisions of this act.

9. Electronic Site: The domain where data are made available on the information network through a specific address.

10. Hacking: Sighting or obtaining information without a valid legal justification.

Article 2

This act aims at controlling IT crimes by identifying these crimes and penalties applied to each of them in order to realize the following:

1. Help realize information security;

2. Preserve the rights of the lawful use of computers and information networks;

3. Protect the public interest, morals and ethics; and
4. Protect national economy.

Article 3

A penalty of imprisonment for a period not exceeding one year and a fine not exceeding five hundred thousand Saudi Riyals or either penalty shall be applied to any person who commits any of the following IT crimes:

1. Any person who eavesdrops, receives or intercepts anything sent through the information network or computer systems;
2. Unlawful access for threatening or harassing a person to make him do or stop him from doing something even if doing or stopping from doing that thing is lawful;
3. Unlawful access to an electronic site to change the designs, damage, amend or make use of the address of the said site;
4. Trespassing on the private life of a person through the abuse of camera mobile phones or the like; and
5. Blackmailing or harming others through different information technology means.

Article 4

A penalty of imprisonment for a period of not more than three years and a penalty of not more than two million Saudi Riyals or either penalty shall be applied to any person who commits any of the following IT crimes:

1. Robbing for himself or for others of a movable property or document or signing the said document through racketeering or a pseudo name or an invalid personality; and
2. Accessing without a valid legal justification to banking or credit data or the data related to the ownership of financial instruments to obtain data, information, property or services;

Article 5

A penalty of imprisonment for a period of not more than four years and a penalty of not more than three million Saudi Riyals or either penalty shall be applied to any person who commits any of the following IT crimes:

1. Unlawful access to cancel, delete, destroy, leak, damage, change or republish private data;
2. Damaging, stopping or destroying information network or deleting, canceling, leaking, or amending existing or used software and data; and
3. Hampering access to, causing interference for or damaging the service by any means whatsoever.

Article 6

A penalty of imprisonment for a period of not more than five years and a penalty of not more than six million Saudi Riyals or either penalty shall be applied to any person who commits any of the following IT crimes:

1. Producing, preparing, transmitting or storing anything that may infringe on public order, religious values, public ethics or private life through the information network or any computer system;
2. Creating or publishing a site on the information network or a computer system for trading in human beings or facilitating the process of trading in human beings;
3. Creating, publishing or marketing materials and data related to pornography networks, gambling or things that harm public morals; and
4. Creating or publishing a site on the information network or a computer system for drug or psychotropic substances, trafficking and marketing them, ways of abuse or facilitating trading thereof.

Article 7

A penalty of imprisonment for a period of not more than ten years and a penalty of not more than five million Saudi Riyals or either penalty shall be applied to any person who commits any of the following IT crimes:

1. Creating or publishing a site for terrorist organizations on the information network or any computer system to facilitate communications with the leaderships of such organizations or any of their members, marketing or financing their ideologies or publishing methods of producing burning devices, explosives or any other device used in terrorist activities; and

2. Unlawful access to an electronic site or an information system either directly or through the information network or a computer system to obtain data that is bound to infringe on internal or external security of the state or its national economy.

Article 8

The penalty of imprisonment or fine shall not be less than half the maximum if the crime is associated with any of the following cases:

1. If the culprit commits the crime through an organized gang,
2. If the culprit occupies a public post and the crime is related to the said post or if he commits the crime by abusing his authority or post,
3. Deceiving or misusing minors and the like, and
4. If previous local or foreign sentences are issued against the culprit for similar crimes.

Article 9

Any person who entices, helps or agrees with others to commit any of the crimes provided for in this act if the crime is then committed based on such enticement, help or agreement shall be penalized in such a way that the penalty shall not exceed the maximum penalty prescribed for the crime and not to exceed half the maximum penalty if the original crime has not taken place.

Article 10

Any person who attempts to commit any of the crimes provided for in this act shall be penalized in such a way that the penalty shall not exceed half the maximum prescribed penalty.

Article 11

The court having jurisdiction may relieve from these penalties any culprit who may inform the concerned authority of the crime before it comes to its attention and before the damage takes place. However, if the information is provided after knowing finding about the crime, the relief should be based on the fact that the information leads to arresting the other culprits if they are more than one or seizing the tools used in committing the crime.

Article 12

The application of this act shall not be in prejudice to the provisions contained in the relevant regulations especially those related to the rights of intellectual property and relevant international agreements which the Kingdom is a party thereto.

Article 13

Without prejudice to the rights of bona fide persons, a judgment shall be issued to confiscate the systems, software or media used in committing any of the crimes provided for in this act or the amounts of money earned from them. It may also be judged to close the electronic site or the service provider site terminally or temporarily as long as it is a place for committing any of the said crimes and as long as the crime is committed with the knowledge of its owner.

Article 14

The Communications and IT Commission, according to its responsibilities, shall provide technical support to the concerned security authorities during the stages of pinpointing and investigating crimes and during trials.

Article 15

The General Prosecutor Commission shall undertake investigation and pleading with regard to the crimes provided for in this act.

Article 16

This act shall be published in the official gazette and shall come into effect one hundred and twenty days after the date of publication.